

---

**Before the  
DEPARTMENT OF COMMERCE  
Internet Policy Task Force**

	)	
	)	
In the Matter of	)	
	)	
Commercial Data Privacy and	)	Docket No. 100402174-0175-01
	)	
Innovation in the Internet Economy:	)	
	)	
A Dynamic Policy Framework	)	
	)	

---

**COMMENTS OF TECHAMERICA**

---

Chris Wilson  
Director and Counsel, E-Commerce and Telecommunications  
TECHAMERICA  
601 Pennsylvania Ave, NW  
North Building, Suite 600  
Washington, D.C. 20004  
(202) 682-4451

January 28, 2011

---

TechAmerica hereby submits these comments to the Department of Commerce (“Department”) in response to the Department’s green paper entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (“Privacy Green Paper”).<sup>1</sup> TechAmerica’s members have a vested interest in the success and future of the Internet and TechAmerica is pleased to be able to file comments on their behalf in this proceeding.

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation for the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, TechAmerica is the industry’s largest advocacy organization and is dedicated to helping members’ top and bottom lines. It is also the technology industry’s only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of the American Electronics Association (AeA), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics and Information Association (GEIA).

TechAmerica’s members include: manufacturers and suppliers of broadband networks and equipment; consumer electronics companies; ICT hardware companies; software and application providers; systems integrators; Internet and e-commerce

---

<sup>1</sup> Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework, The Department of Commerce Internet Policy Task Force, released Dec. 16, 2010, *available at* <http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf> (“Privacy Green Paper”).

---

companies; Internet service providers; information technology government contractors; and information technology consulting and sourcing companies.

TechAmerica welcomes this opportunity to provide the Department's Internet Policy Task Force with a viewpoint shared by such a diverse membership.

## **Introduction**

TechAmerica applauds the Department for its formulation of its Privacy Green Paper. The Privacy Green Paper provides much thoughtful input into the creation of a comprehensive U.S. privacy policy and TechAmerica appreciates the Department's willingness to listen to the technology industry's viewpoints regarding commercial online privacy. To be sure, consumer privacy has been and remains today a core focal point for all participants in the Internet industry, regardless of whether or not they interact with a consumer directly.

TechAmerica generally supports the Department's four key policy recommendations: 1) enhancing consumer trust online through recognition of revitalized Fair Information Practice Principles (FIPPs); 2) developing voluntary and enforceable privacy codes of conduct; 3) promoting global interoperability; and 4) ensuring nationally consistent security breach notification rules.

TechAmerica believes that, if implemented properly, these policy recommendations will facilitate the free flow of goods, services, and speech online while at the same time ensuring that consumers can trust that their information is collected, used, and stored prudently.

TechAmerica is especially heartened in the Department's recognition of the "dynamic nature of both technologies and markets" and the need to promote "continued

---

innovation over time.”<sup>2</sup> Technological innovation has flourished, especially over the last two decades, largely because of public policies that avoid prescriptive rules regulating Internet commerce while respecting technology’s ability to enhance and improve consumers’ lives. In this vein, TechAmerica believes strongly that technology is essential to protecting consumer privacy. The Department recognizes this notion in its Privacy Green Paper and TechAmerica applauds it for doing so. In responding to the Department’s “Questions for Further Discussion,” TechAmerica appreciates the opportunity to expound further on the virtues of technology as a consumer privacy enhancer.

Indeed, as President Obama emphasized in his State of the Union Address, it is essential that the U.S. remain an industry leader in the technology sector, including with regard to the Internet and communications and that it increase its competitiveness internationally in technological development. This will solidify the position of the U.S. as a global leader in technological innovation and add high-value jobs at a time when those jobs are most crucial for our growth and well-being.

**Federal Privacy Framework Based on Fair Information Practice Principles Driven by Self-Regulation**

The Department asks a series of questions regarding the implementation of “an expanded set of Fair Information Practice Principles (FIPPs).”<sup>3</sup> TechAmerica is pleased to respond.

Specifically, TechAmerica believes that baseline commercial privacy principles, such as comprehensive FIPPs, need not be enacted by statute or regulation. Rather,

---

<sup>2</sup> Privacy Green Paper at 3.

<sup>3</sup> Privacy Green Paper at 70.

---

TechAmerica believes that a federal privacy framework incorporating expanded FIPPs should be encouraged and implemented via industry-driven codes of conduct and self-regulation. This approach will provide industry with the necessary flexibility to innovate and adjust its privacy practices in conjunction with evolving technologies and consumer expectations. Such an approach will also ensure that any framework is technologically neutral, which TechAmerica believes is a key component of any effective privacy framework.

With regard to enforcement of an expanded FIPPs federal privacy framework, TechAmerica believes the Federal Trade Commission (FTC) can enforce such a framework pursuant to its current authority under Section 5 of the Federal Trade Commission Act. Further, State Attorneys General may also enforce industry-driven codes of conduct as they currently do today. Of course, as a supporter of industry-driven privacy regimes, TechAmerica believes that enforcement by non-governmental self-regulatory organizations, such as TRUSTe, BBBOnline, and CARU, is certainly welcome and serves as the first line of assurance that a federal framework of expanded FIPPs is sufficiently implemented.

Concerning certain FIPPs, TechAmerica agrees with the Department that, in order to facilitate consumer awareness and understanding, a single federal privacy framework should promote industry transparency in the practices and procedures used to collect, store and use consumer information where warranted because of the sensitivity of the data and its use. Certainly, for example, consumer-facing companies should provide individuals with clear, concise notices that outline the type of information

---

collected, the purpose for which the information is collected, and how that information is handled by the business entity.

Indeed, TechAmerica believes that purpose specifications are an important method for protecting commercial privacy. However, in implementing a federal privacy framework, industry must be allowed to specify purpose and use in a sufficiently general manner to permit ongoing innovation. To be sure, it is important to note that FIPPs are high-level principles whose application varies significantly based on the type of data in question and the context in which it is used. Of course, organizations should be accountable to consumers regarding whether information is collected and used in accordance with stipulated policies, but any use of information that may be inconsistent with a purpose specification should not lead to immediate sanction. Rather, an organization should be provided an opportunity to remedy the problem.

With regard to the use of Privacy Impact Assessments (PIAs), TechAmerica believes PIAs are useful ways for companies to assess internal operations. However, as consumer-facing documents, PIAs should not be mandated, as they would unnecessarily burden companies, could be used for nefarious purposes, and are not likely to be more transparent than simplified privacy notices.

**If Legislation or Regulation is Considered, It Should Provide for a Safe Harbor and Expressly Disclaim a Private Right of Action**

While TechAmerica believes a legislative or regulatory regime is not necessary in order to implement a single federal framework based on an expanded set of FIPPs, to the extent there is consideration of baseline consumer privacy legislation or regulation, TechAmerica believes that it should provide for a safe harbor for the adoption of widely accepted industry best practices, as discussed above. TechAmerica applauds the

---

Department for recommending multi-stakeholder efforts instead of legislation. Indeed, a safe harbor will provide industry with the necessary assurances that it can provide innovative uses of consumer information, as well as innovative solutions to privacy protection, without the need for heavy-handed and prescriptive regulation.

The Department specifically asks if there were to be “baseline commercial data privacy legislation” whether it should include a private right of action. TechAmerica does not believe baseline privacy legislation is necessary in order to implement a single federal framework based on expanded FIPPs. However, to be responsive to the Department, TechAmerica responds to the issue of a private right of action by stating that it strongly opposes the inclusion of this element in any baseline commercial privacy bill or industry-led federal framework. The primary result of private rights of action is often the enrichment of the plaintiffs’ bar rather than the protection of consumers’ data. Moreover, many of the goals expounded by the Privacy Green Paper, including advancing innovation and increased transparency are not served through private rights of action. Exposing industry participants, especially innovative risk-taking technology industry participants, to potential private party liability will only stifle innovation as companies will cease developing cutting-edge technologies that may utilize personally identifiable information for consumer benefit.

### **Privacy Policy Office (“PPO”) and Global Harmonization**

TechAmerica supports the creation of a Privacy Policy Office (“PPO”) in the Department of Commerce in order to facilitate innovative privacy practices across industries. The PPO should facilitate the creation of a multi-stakeholder self-regulatory program that implements a federal privacy framework based on an expanded set of

---

FIPPs. The PPO can not only encourage more businesses to participate in the self-regulatory process, but it can also serve, possibly, as a needed voice internationally for U.S. industry with respect to worldwide policies on data protection. TechAmerica believes that the Department should advocate for a global framework consistent with U.S. privacy standards. Global interoperability should promote, not impede, economic competition and innovation. The PPO could serve as the necessary voice within the Department for such an advocacy role. TechAmerica supports the notion that the PPO can serve as the point of contact for both industry and international partners, provide effective leadership and coordination on privacy policy considerations, and discuss technology development and business and government needs.

### **Security Breach Notification**

TechAmerica supports a national security and data breach notification regime that provides for a streamlined approach to notification requirements based on risk of harm to the individual(s) whose personally identifiable information may have been breached. The Data Accountability and Trust Act (H.R. 2221) that passed the House of Representatives in the 111<sup>th</sup> Congress is a good example of the factors that such a national regime should entail, including (a) pre-emption of state laws in order to provide for harmonization; (2) applicability to all types of entities: industry, government, non-profit organizations, academic organizations, etc.); (3) notification requirements based on risk of harm; and (4) exemption from notification for entities that take preventive measures to render data unreadable, unusable, or undecipherable and thereby reduce the risk of harm.



---

## **Conclusion**

TechAmerica appreciates the Department's efforts in creating its "Dynamic Policy Framework." TechAmerica especially applauds the Department's recognition of the "dynamic" nature of technologies and the need to encourage continued innovation over time. Indeed, the Framework, when implemented by industry in consultation with the Department's PPO, will create a national uniform privacy regime that incentivizes innovation, empowers consumers, and preserves industry's ability to provide informational and network security.

As the Department continues to examine this issue, TechAmerica welcomes the opportunity to assist the Department in ensuring that consumer interests remain properly balanced with industry's innovation needs.